Counting Subrings of $\mathbb{Z}^n$ of index k for small n

Nathan Kaplan
Harvard University
Cambridge, MA
nkaplan@math.harvard.edu

Ramin Takloo-Bighash
University of Illinois at Chicago
Chicago, IL
rtakloo@math.uic.edu

August 13, 2010

Abstract

In this article we investigate subring growth of $\mathbb{Z}^n$ for small n using p-adic integration.

To the memory of Fritz Grunewald

Contents

1 Introduction

Let $\mathbb{Z}^n$ be the ring of n-tuples of integers equipped with componentwise addition and multiplication. Namely for $v = (v_1, \dots, v_n), w = (w_1, \dots, w_n) \in \mathbb{Z}^n$, we set

$$v + w = (v_1 + w_1, \dots, v_n + w_n),$$

$$v \circ w = (v_1 w_1, \dots, v_n w_n).$$

The goal of this paper is to investigate the rate of growth of the number of subrings of $\mathbb{Z}^n$ of bounded additive index. Namely, for any real number $B > 0$, we set

$$N_n(B) := \left|\{R \leq \mathbb{Z}^n; [\mathbb{Z}^n : R] \leq B\}\right|$$

and we wish to determine the asymptotic behavior of $N_n(B)$ as $B \to \infty$. This problem is motivated by the the problem of determining the distribution of orders in number fields as asked by Bhargava ([9]). In the case of $\mathbb{Z}^n$ Bhargava conjectures the following:

Conjecture 1 (Bhargava)**.** *Let $f_n(k)$ be the number of subrings of $\mathbb{Z}^n$ of additive index equal to k. Then for n odd,*

$$f_n(k) = O(k^{\frac{n-1}{6}+\epsilon}),$$

and for n even,

$$f_n(k) = O(k^{\frac{n^2-2n}{6n-8}+\epsilon}).$$

This would have the following consequence:

Conjecture 2 (Bhargava)**.** *For n odd,*

$$N_n(B) = O(B^{\frac{n-1}{6}+1+\epsilon}),$$

and for n even,

$$N_n(B) = O(B^{\frac{n^2-2n}{6n-8}+1+\epsilon}).$$

Determining the asymptotic behavior of $N_1(B)$ and $N_2(B)$ is trivial. In this paper we prove the following theorem:

Main Theorem 1. *Let $n \leq 5$. There is a positive real number C_n such that*

$$N_n(B) \sim C_n B (\log B)^{\binom{n}{2}-1}$$

as $B \to \infty$.

This theorem verifies a strong form of Conjecture 2 for n up to 5. The method we present here gives error estimates as well (see Theorems 2, 7 and 13). Here we should point out that for $n = 3, 4$ our theorem is a consequence of Propositions 6.2 and 6.3 of [9]. The case $n = 5$ seems to be new. For general n we prove the following "easy estimate":

Main Theorem 2. *Suppose $n \geq 6$. Then for any $\epsilon > 0$ we have*

$$N_n(B) = O_\epsilon(B^{\frac{n}{2}-\frac{21}{20}+\epsilon})$$

as $B \to \infty$.

We note that the number of sublattices of $\mathbb{Z}^n$ of index bounded by B grows like B^n.

Here we will use p-adic integration and Tauberian theorems as suggested by the seminal paper [6]. The method of p-adic integration, extending the techniques of [7, 3], has been quite successfully applied to the study of counting subgroups of nilpotent groups (see, for example, [5, 4, 6] and the references therein). Following [6] we write the counting zeta function of subrings as an Euler product. Each Euler factor then is expressed as a *Cone integral* ([5]).

Cone integrals of the type obtained here are in principle computable. On one hand there is the method of resolution of singularities and on the other hand the elimination of quantifiers in non-archimedean fields and both of these methods have successfully been applied to various problems (see e.g. [3, 4] as well as [8] where the case $n = 3$ of our main theorem has been proved using resolution of singularities). Neither of these methods can be applied to our specific problem for general n in any obvious fashion. This is due to the fact that our cone integral is too complicated (see Sections 5 and 7). In general there is no effective algorithm to eliminate quantifiers for a complicated p-adic domain, and resolution of singularities, while in principle computationally tractable, is dreadful for domains of the type considered here. The domain needed to study $\mathbb{Z}^n$ would involve about n^3 inequalities of the form $v_p(f(\underline{x})) \leq v_p(g(\underline{x}))$ with $\underline{x}$ a vector of variables of length about n^2, and f, g ranging over polynomials with integer coefficients of degrees 2 to n.

Our observation here is that if one is just interested in determining the asymptotic behavior of $N_n(B)$ then one actually does not need to explicitly compute the cone integrals, provided that one can determine the main term that dominates the behavior of the zeta function. We use the geometry of the domain of integration to decide what portion of the domain would not contribute to the asymptotic behavior without having to deal with the actual subrings (Compare this with [9]). In this regard, our argument is much more simple minded than the works that it follows ([2, 9, 11]). We have explained our approach in the simplest non-trivial case of $\mathbb{Z}^3$ in Section 4. This approach has the advantage that the proof for $n = 3, 4$ is simple, and it allows us to capture $n = 5$. Here the actual work lies in estimating volumes of certain p-adic sets. The main merit of our "adelic" approach is that the ring $\mathbb{Z}$ can be replaced by the ring of integers of any number field, and also that, at least in principle, the ring $\mathbb{Z}^n$ can be replaced by the ring of integers of any cubic, quartic, or quintic extension of $\mathbb{Q}$.

The argument presented in this paper is at the end of the day ad hoc. It would be very interesting to interpret the growth of the number of subrings as a question about group actions and counting appropriate group theoretic objects in the spirit of [12]. The conjectural functional equation of [9] is an indication that such a connection should exist. We have not been successful finding such an interpretation, however. We pose this as a challenge to the interested reader.

This work owes a great deal of intellectual debt to Ricky Liu's paper [9]. This paper has its genesis in the Princeton senior thesis [8]. The first author wishes to acknowledge support from a National Science Foundation Graduate Research Fellowship. The second author wishes to acknowledge support from the National Science Foundation (Award number DMS-0701753). In the course of the preparation of this work we benefited from conversations with Manjul Bhargava, Simon Kochen, Ricky Liu, Alice Medvedev, and Alireza Salehi-Golsefidi.

The paper is organized as follows. The basic strategy of the proof of the main theorem is presented in Section 2 with technical details postponed to later sections. In Section 3 we collect several lemmas used in estimating volumes. Section 4 contains the treatment of the simple case of $\mathbb{Z}^3$. We include this simple case to illustrate the method. In Sections 5 and 7 we give bounds for the volumes of our domains for $n = 4$ and $n = 5$, respectively. These bounds are then used in Sections 6 and 8 to establish Theorems 6 and 12 which are the main technical ingredients of the proof of the Main Theorem 1. Main Theorem 1 is contained in Theorems 2, 7, and 13. The proof of the Main Theorem 2 is presented in Section 9. Section 10 contains the statements of the Tauberian theorems we use in this work.

2 Preliminaries

2.1 Multiplicative sublattices

A sublattice $L \subset \mathbb{Z}^n$ is multiplicative if it is closed under componentwise multiplication in $\mathbb{Z}^n$. A subring is a multiplicative lattice that contains the identity element $1 = (1, \ldots, 1)$. We set $f_n(k)$ to be the number of subrings of $\mathbb{Z}^n$ of index k. We also let $t_n(k)$ to be the number of multiplicative sublattices of $\mathbb{Z}^n$ of index k. Then

Proposition 1 (Proposition 2.3 of [9]). *For each $k \geq 1$, we have*

$$t_n(k) = f_{n+1}(k).$$

As a consequence of this proposition we find that for $n \geq 2$

$$N_{n+1}(B) = \sum_{k=1}^{[B]} t_n(k).$$

We then set

$$\mathcal{Z}_n(s) := \sum_{n \geq 1}^{\infty} \frac{t_n(k)}{k^s}.$$

Since $t_n(k)$ is certainly bounded by the number of all sublattices of index k in $\mathbb{Z}^n$, and the latter grows at most like a polynomial of k (e.g. Prop. 1.1 of [6]), we conclude that for $\Re s$ large the series $\mathcal{Z}_n(s)$ is absolutely convergent. It is not hard to see that the function $t_n(k)$ is a multiplicative function of the variable k, i.e. $t_n(k_1 k_2) = t_n(k_1) t_n(k_2)$ whenever $\gcd(k_1, k_2) = 1$. Our Theorem will then follow, via an application of a Tauberian theorem, from the study of the analytic properties of the zeta function $\mathcal{Z}_n(s)$.

We can similarly define subrings and multiplicative sublattices of $\mathbb{Z}_p^n$. We will set $t_n(k, p)$ be the number of multiplicative $\mathbb{Z}_p$-sublattices in $\mathbb{Z}_p^n$. Clearly, $t_n(k, p) = 0$ unless k is a p-power. We also set

$$\mathcal{Z}_n(s, p) = \sum_{k=1}^{\infty} \frac{t_n(k, p)}{k^s}.$$

The function $\mathcal{Z}_n(s, p)$ too converge absolutely for $\Re s$ large. It is an observation of §3 of [6] that

$$\mathcal{Z}_n(s) = \prod_{p \text{ prime}} \mathcal{Z}_n(s, p).$$

We can represent any lattice L as a lower triangular matrix with entries in $\mathbb{Z}_p$,

$$M = \begin{pmatrix} x_{11} & 0 & \ldots & 0 \\ x_{21} & x_{22} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_{n1} & \ldots & \ldots & x_{nn} \end{pmatrix}.$$

Here the lattice is generated by the row-vectors of the matrix. Following §3 of [6] we denote by $\mathcal{M}_n(p)$ the set of all lower triangular matrices whose rows generate a multiplicative sublattice of $\mathbb{Z}_p^n$. Let $v_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ denote the i^{th} row. We want L to be both multiplicatively and additively closed. Therefore we must have $v_j \circ v_k = \sum_{i=1}^{n} \alpha_i v_i$, for $\alpha_i \in \mathbb{Z}_p$ for each i. The following proposition shows that each of the local zeta functions $\mathcal{Z}_n(s, p)$ can be represented as a *cone integral*.

Proposition 2 (Proposition 3.1 of [6]). *For every prime p,*

$$\mathcal{Z}_n(s,p) = (1-p^{-1})^{-n} \int_{M \in \mathcal{M}_n(p)} |x_{11}|_p^{s-n} |x_{22}|_p^{s-(n-1)} \cdots |x_{nn}|_p^{s-1} |dv|,$$

where $|dv|$ is the additive Haar measure of the p-adic lower triangular matrices.

Remark 1. We note that this proposition combined with standard properties of cone integrals readily verifies the rationality conjecture in the last section of [9].

Example. Let's consider $n = 1$. A 1×1 matrix $M = (x_{11})$ is in $\mathcal{M}_1(p)$ if and only if $v_p(x_{11}) \geq 0$. So the proposition tells us that

$$\mathcal{Z}_1(s,p) = (1-p^{-1})^{-1} \int_{\mathbb{Z}_p} |x_{11}|_p^{s-1} |dx_{11}|$$

A standard computation then shows that $\mathcal{Z}_1(s) = \zeta(s)$.

For $n = 2, 3, 4$, we will give an explicit description of $\mathcal{M}_n(p)$ in Sections 4, 5 and 7.

If $\underline{k} = (k_1, \ldots, k_n)$ is an n-tuple of non-negative integers, we set

$$\mathcal{M}_n(p;\underline{k}) = \left\{ M = \begin{pmatrix} p^{k_1} & 0 & \ldots & 0 \\ x_{21} & p^{k_2} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_{n1} & \ldots & x_{n\,n-1} & p^{k_n} \end{pmatrix} \in \mathcal{M}_n(p) \right\}.$$

We define $\mu_p(\underline{k})$ to be the $\frac{n(n-1)}{2}$-dimensional volume of $\mathcal{M}_n(p;\underline{k})$. It is then easy to see that

$$\mathcal{Z}_n(s,p) = \sum_{\substack{\underline{k}=(k_1,\ldots,k_n) \\ k_i \geq 0, \forall i}} p^{\sum_{i=1}^n (n-i)k_i} p^{-s\sum_{i=1}^n k_i} \mu_p(\underline{k}). \tag{1}$$

Intuitively what this means is that we have multiplied the rows by units to make the diagonal entries a p-power. We note that this does not change the lattice generated by the rows.

2.2 The idea of the proof

The strategy is very simple. We start by writing

$$\mathcal{Z}_n(s) = \prod_p \mathcal{Z}_n(s,p).$$

Since each $\mathcal{Z}_n(s,p)$ is a power series in p^{-s} we write

$$\mathcal{Z}_n(s,p) = 1 + \sum_{k=1}^{\infty} a_n(k;p) p^{-ks}.$$

The following is easy to prove

Lemma 1. *We have*

$$a_n(1;p) = \binom{n+1}{2}.$$

For a proof see [9] Proposition 1.1. The quantity $a_n(1;p)$ is equal to $f_{n+1}(p)$ of that reference. We now apply Theorem 16. Our main theorem is then proved if we can show the following.

Lemma 2. *Let $n = 3, 4, 5$. There is an $\epsilon > 0$ such that for $\Re s = \sigma > 1 - \epsilon$ we have*

$$\sum_p \sum_{k=2}^{\infty} \frac{|a_n(k;p)|}{p^{k\sigma}} < \infty.$$

Since by Equation (1)

$$a_n(k;p) = \sum_{\substack{\underline{k}=(k_1,\ldots,k_n) \\ \sum_i k_i = k}} p^{\sum_i (n-i)k_i} \mu_p(\underline{k}),$$

in order to prove the lemma we need to estimate $\mu_p(\underline{k})$. For $n = 3$ this is easy as is shown in Section 4. The lemma for $n = 4, 5$ follows from Theorem 6 and Theorem 12 respectively. These results are stated in Theorems 2, 7, and 13.

3 General facts about volumes

We begin with some lemmas. Let U_p denote the set of units of $\mathbb{Z}_p$.

Proposition 3. *For fixed $y, z \in \mathbb{Z}_p$, $k \geq 0$ the volume of $x \in \mathbb{Z}_p$ such that $v_p(xy - z) \geq k$ is at most $p^{-(k - v_p(y))}$.*

Proof. We first note that for $y = 1$, the volume of x such that $v_p(x - z) \geq k$ is p^{-k}, since we are just fixing the first k digits in the p-adic expansion of x to coincide with those of z. Similarly, for any unit $u \in U_p$ we have that the volume of x such that $v_p(ux - z) \geq k$ is p^{-k}.

Recall that for $\alpha, \beta \in \mathbb{Z}_p$, if $v_p(\alpha) \neq v_p(\beta)$ then $v_p(\alpha - \beta) = \min\{v_p(\alpha), v_p(\beta)\}$. We see that if $v_p(z) < k$ and $v_p(y) > v_p(z)$, then clearly $v_p(xy - z) = v_p(z) < k$ for any value of x. If $v_p(z) \geq k$, then $v_p(xy - z) \geq k$ if and only if $v_p(xy) \geq k$ which holds if and only if $v_p(x) \geq k - v_p(y)$. This holds on a set of volume at most $p^{-(k - v_p(y))}$ if $k \geq v_p(y)$ and on a set of volume 1 if $v_p(y) \geq k$.

Now if $v_p(z) < k$ and $v_p(y) \leq v_p(z)$ then we can write $y = p^{v_p(y)}u$ for some unique unit $u \in U_p$, and $z = p^{v_p(y)}z'$ for some unique $z' \in \mathbb{Z}_p$. We have $v_p(xy - z) \geq k$ if and only if $v_p(xu - z') \geq k - v_p(y)$, which holds on a set of volume at most $p^{-(k - v_p(y))}$. □

Proposition 4. *For fixed values of $k, l \geq 0$, the volume of $x \in \mathbb{Z}_p$ such that*

$$k \leq v_p(x) + v_p(x - p^l),$$

is at most $2p^{-\lceil k/2 \rceil}$.

Proof. We will consider two cases. First suppose that the inequality holds and $v_p(x) \geq \lceil k/2 \rceil$. This clearly holds on a set of volume at most $p^{-\lceil k/2 \rceil}$. Now suppose that the inequality holds and $v_p(x) < \lceil k/2 \rceil$. We must have $v_p(x - p^l) \geq k - v_p(x) > k - \lceil k/2 \rceil$. This means that $v_p(x - p^l) \geq \lceil k/2 \rceil$, and this holds on a set of volume at most $p^{-\lceil k/2 \rceil}$. Therefore this inequality holds on a set of volume at most $2p^{-\lceil k/2 \rceil}$. □

We point out that in the most general possible case it is not possible to improve this result by more than a factor of 2. Suppose $l \geq \lceil k/2 \rceil$. Then $v_p(x) + v_p(x - p^l) \geq k$ if and only if $v_p(x) \geq \lceil k/2 \rceil$, which holds on a set of volume at most $p^{-\lceil k/2 \rceil}$. However, in some cases we can say something stronger.

Proposition 5. *For fixed values of $k, l \geq 0$, the volume of $x \in \mathbb{Z}_p$ such that*

$$k \leq v_p(x) + v_p(x - p^l),$$

is at most $2p^{-(k-l)}$.

Proof. We consider two cases, when $v_p(x) = l$ and when $v_p(x) \neq l$. In the first case we must have $v_p(x - p^l) \geq k - l$, and in the second case we have $v_p(x) \geq k - l$. □

Proposition 6. *For fixed $z \in \mathbb{Z}_p$, the combined volume of $x, y \in \mathbb{Z}_p^2$ such that $v_p(xy - z) \geq k$ is at most $(k + 1)p^{-k}$.*

Proof. If $v_p(y) \geq k$, then there are two cases. Either $v_p(z) \geq k$ in which case any x will work, or $v_p(z) < k$ in which case no x works. So assume $0 \leq v_p(y) < k$. Then given y with $l = v_p(y)$ we need x such that $x \in p^{-l}(p^k\mathbb{Z}_p + z)$. So the total volume is

$$\sum_{l=0}^{k-1} p^{-l}\mathrm{vol}\left(p^{-l}(p^k\mathbb{Z}_p + z)\right) = kp^{-k}.$$

□

Proposition 7. *For any fixed $z \in \mathbb{Z}_p$, the combined volume of $x, y \in \mathbb{Z}_p^2$ such that $v_p(x(y-z)) \geq k$ is at most $(k + 1)p^{-k}$*

Proof. This proposition is very similar to the previous one. We have $v_p(x) \geq k$ on a set of volume p^{-k}. Suppose that this does not hold and set $v_p(x) = m$. We see that for any fixed z the volume of y such that $v_p(y - z) \geq k - m$ is $p^{-(k-m)}$. Summing over the k possible values of m gives the result. □

Proposition 8. *Suppose $z \in \mathbb{Z}_p$, $k, l \geq 0$ are given. Then the volume of $x \in \mathbb{Z}_p$ such that*

$$v_p(x(x - p^l) - z) \geq k$$

is bounded by $2p^{-\lceil k/2 \rceil}$.

Proof. If there is no such x then the volume is zero and there is nothing to prove. So let's assume that the volume is non-zero. Let $y = p^l$. If $v_p(x(x - y) - z) \geq k$, then $x + t$ also satisfies the same inequality whenever $v_p(t) \geq k$. This means that we can assume that x is determined modulo p^k. So the problem is this, given y and z modulo p^k, determine the number of x modulo p^k such that $x(x - y) - z \equiv 0 \mod p^k$. If this number is N, the volume of our domain is going to be $N.p^{-k}$. So suppose $X, X + u$ are both solutions of the congruence

$$x(x - y) \equiv z \mod p^k.$$

This implies that u satisfies the congruence

$$u^2 + u(2X - y) \equiv 0 \mod p^k.$$

We count the number of solutions u of this congruence equation. Suppose $2X - y \equiv p^s q \mod p^k$ with $q = 0$ or $(q, p) = 1$. First we treat the case where $(q, p) = 1$. Write $u = p^r m \mod p^k$ with $(m, p) = 1$. Then $u^2 \equiv p^{2r}m^2 \mod p^k$. Then we get

$$p^{2r}m^2 \equiv -p^{s+r}qm \mod p^k.$$

- If $2r < k$, then $s + r = 2r$, and as a result $s = r$. This then implies further that $m^2 \equiv -qm \mod p^{k-2r}$. Consequently $m \equiv -q \mod p^{k-2r}$. This means

$$m = -q + bp^{k-2r} \mod p^k$$

for some b. Then

$$u \equiv p^r m \equiv -qp^r + bp^{k-r} \mod p^k.$$

Since $r = s$

$$u \equiv y - 2X + bp^{k-s} \mod p^k$$

with b having p^s possibilities. This gives p^s possibilities for t. Sine $2s < k$, we get $s \leq \lfloor k/2 \rfloor$. As a result in this situation we have at most $p^{\lfloor k/2 \rfloor}$.

- If $2r \geq k$, then we get $u^2 \equiv 0 \mod p^k$. We note that this is the same as taking $q = 0$. Here any solution u will be of the form

$$a_r p^r + a_{r+1} p^{r+1} + \cdots + a_{k-1} p^{k-1}$$

with $2r \geq k$, i.e. $r \geq \lceil k/2 \rceil$. There are at most $p^{k - \lceil k/2 \rceil}$ choices for u.

Adding up we have at most

$$p^{\lfloor k/2 \rfloor} + p^{k - \lceil k/2 \rceil}$$

many solutions. Multiplication with p^{-k} gives the result. □

Proposition 9. *Suppose $z \in \mathbb{Z}_p$, $k, l \geq 0$ are given. Then there is a constant C, which for odd p maybe taken to be 6, such that the volume of $x \in \mathbb{Z}_p$ satisfying*

$$v_p(x(x - p^l) - z) \geq k$$

is bounded by $Cp^{-(k-l)}$ except when $p = 2$ and $v_2(z) = 2l - 2 < k$. In this exceptional situation:

1. *If $v_2(z + 2^{2l-2}) \geq k$, the volume is bounded by $2^{-\lceil k/2 \rceil}$, and this is the best bound possible.*

2. *If $v_2(z + 2^{2l-2}) < k$ is odd, the volume is zero.*

3. *If $v_2(z + 2^{2l-2}) < k$, the volume is bounded by*

$$8 \left| z + 2^{2l-2} \right|^{-1/2} 2^{-k}.$$

Proof. The proposition will have no content unless $l < k$. First we consider the case where p is odd. We recognize two basic cases:

1. If $v_p(z) \geq k$, then we have $v_p(x(x - p^l)) \geq k$. In this case the result follows from Proposition 5.

2. If $v_p(z) < k$, then our inequality can be valid only when $v_p(x(x - p^l)) = v_p(z)$. Since $v_p(z) < k$, we write $z = \zeta p^u$ with $u < k$. We wish to have

$$v_p(x(x - p^l) - \zeta p^u) \geq k$$

and we need $v_p(x) + v_p(x - p^l) = u$.

- If $v_p(x) > l$, then we must have $v_p(x) + l = u$, and as a result $u - l > l$ which means $u > 2l$. Write $x = \epsilon p^{u-l}$. Then we need $v_p(\epsilon p^{u-l}(\epsilon p^{u-l} - p^l) - \zeta p^u) \geq k$. This implies $v_p(\epsilon(\epsilon p^{u-2l} - 1) - \zeta) \geq k - u$. This is a quadratic equation in ϵ with at most two solutions modulo p. Hensel's lemma says that the volume of ϵ satisfying this last inequality is at most $2p^{-(k-u)}$. The volume for x is then at most $2p^{-(u-l)}.p^{-(k-u)} = 2p^{-(k-l)}$.

- (*) If $v_p(x) < l$, then $2v_p(x) = u$, which means u is even and $u < 2l$. Write $x = \epsilon p^{u/2}$. Then we need $v_p(\epsilon p^{u/2}(\epsilon p^{u/2} - p^l) - \zeta p^u) \geq k$ which gives $v_p(\epsilon(\epsilon - p^{l-u/2}) - \zeta) \geq k - u$. By Hensel's lemma the volume of such ϵ is at most $2p^{-(k-u)}$. The volume of x is then bounded by $2p^{-(k-u)}.p^{-u/2} = 2p^{-k+u/2} < 2p^{-k+l}$ which is what we want.

- if $v_p(x) = l$, then $x = \epsilon p^l$, and we have $2l + v_p(\epsilon - 1) = u$. This means $u \geq 2l$. Then we need $v_p(\epsilon(\epsilon - 1) - \zeta p^{u-2l}) \geq k - 2l$. An application of Hensel's lemma then says that the volume of ϵ satisfying this inequality is at most $2p^{-(k-2l)}$. Since $x = p^l\epsilon$, the volume of x is at most $2p^{-(k-l)}$.

Now we examine the situation for $p = 2$. Except for the step marked (*) every other step of the proof works verbatim. The argument (*) can be adjusted as follows. We let $r = l - \frac{u}{2}$ and $s = k - u$. Then $r \geq 1$ and we are trying to determine the volume of ϵ unit such that

$$v_2(\epsilon(\epsilon - 2^r) - \zeta) \geq s.$$

for a given unit ζ. Rewrite this inequality as

$$v_2((\epsilon - 2^{r-1})^2 - (\zeta + 2^{2r-2})) \geq s.$$

First we consider the situation for $r \geq 2$. In this case both $\epsilon - 2^{r-1}$ and $\zeta + 2^{2r-2}$ are still units, and without loss of generality we may assume that our inequality has the form

$$v_2(\epsilon^2 - \zeta) \geq s$$

with ϵ, ζ units. Fix an ϵ that satisfies the inequality, and we determine for what values of τ, $\epsilon + \tau$ also satisfies the inequality. The volume of such τ is the volume of ϵ. We have

$$v_2((\epsilon + \tau)^2 - \zeta) = v_2((\epsilon^2 - \zeta) + \tau(\tau + 2\epsilon)).$$

This implies that

$$v_2(\tau(\tau + 2\epsilon)) \geq s.$$

This immediately implies that $v_2(\tau) \geq s - 1$ or $v_2(\tau + 2\epsilon) \geq s - 1$. Consequently the volume of ϵ is bounded by $2.2^{-(s-1)} = 4.2^{-(k-u)}$. The rest of the argument works as before.

Now we consider the case where $r = 1$. In this case the inequality becomes

$$v_2((\epsilon - 1)^2 - (\zeta + 1)) \geq s.$$

There are two cases to consider:
Case I. $v_2(\zeta + 1) \geq s$. In this case we see that $v_2(\epsilon - 1) \geq \lceil s/2 \rceil$ and as a result the volume is $2^{-\lceil s/2 \rceil}$. The volume of x is then seen to be bounded by $2^{-\lceil k/2 \rceil}$.
Case II. $v_2(\zeta + 1) < s$. We write $\zeta + 1 = \gamma.2^{2t}$, with γ a unit (if $v_2(\zeta + 1)$ is odd, we get no ϵ). Then we need to have $v_2(\epsilon - 1) = t$, and we write $\epsilon - 1 = \omega.2^t$. This then implies

$$v_2(\omega^2 - \gamma) \geq s - 2t.$$

The volume of such ω by what we did earlier is bounded by 4.2^{-s+2t}. The volume of ϵ then is bounded by 4.2^{-s+t}. The volume of x is then bounded by $4.2^{-k+l}.2^t$. □

4 $n = 3$

First we determine $\mathcal{M}_2(p)$.

Lemma 3. *$\mathcal{M}_2(p)$ is the collection of matrices*

$$M = \begin{pmatrix} x_{11} & 0 \\ x_{21} & x_{22} \end{pmatrix},$$

with entries in $\mathbb{Z}_p$ such that

$$v_p(x_{21}(x_{21} - x_{22})) \geq v_p(x_{11}).$$

Proof. Let v_1 and v_2 be the first and the second rows of M respectively. Then if the entries are in $\mathbb{Z}_p$ it is clear that $v_1 \circ v_1, v_1 \circ v_2$ are integral linear combinations of v_1, v_2 and vice versa. Now we need $v_2 \circ v_2 = \alpha_1 v_1 + \alpha_2 v_2$ with $\alpha_1, \alpha_2 \in \mathbb{Z}_p$. So $x_{22}^2 = \alpha_2 x_{22}$, which implies $\alpha_2 = x_{22}$. Then $\alpha_1 x_{11} + x_{22} x_{21} = x_{21}^2$, and $\alpha_1 = x_{11}^{-1}(x_{21}^2 - x_{21} x_{22})$. Therefore α_1 is in $\mathbb{Z}_p$ if and only if $v_p(x_{11}) \leq v_p(x_{21}^2 - x_{21} x_{22})$. □

Theorem 1. *If $\sigma > \frac{1}{2}$ the series*

$$\sum_p \sum_{k+l \geq 2} p^k p^{-k\sigma - l\sigma} \mu_p(k, l)$$

converges.

Proof. We divide the series to three subseries:

Case I. $k \geq 0, l \geq 2$. Then by Proposition 4

$$\mu_p(k, l) \leq 2p^{-k/2}.$$

Our subseries is then majorized by

$$\sum_p \sum_{k \geq 0} \sum_{l \geq 2} p^{k/2} p^{-k\sigma - l\sigma}$$

which converges for $\sigma > \frac{1}{2}$.

Case II. $k \geq 2, l = 0$. Then by Proposition 4

$$\mu_p(k, 0) \leq 2p^{-k}$$

and as a result our subseries is majorized by

$$\sum_p \sum_{k \geq 2} p^{-k\sigma}$$

which converges for $\sigma > \frac{1}{2}$.

Case III. $k = 1, l = 1$. By proposition 4

$$\mu_p(1, 1) \leq 2p^{-1}$$

and our subseries is majorized by

$$\sum_p p^{-2\sigma}.$$

This converges for $\sigma > \frac{1}{2}$. □

We have then proved the following theorem:

Theorem 2. *There is a polynomial P_3 of degree 2 such that for all $\epsilon > 0$*

$$N_3(B) = BP_3(\log B) + O(B^{\frac{1}{2}+\epsilon})$$

as $B \to \infty$. For all k

$$f_3(k) = O(k^{\frac{1}{2}+\epsilon}).$$

Proof. The theorem is immediate from Theorems 1, Lemma 1, and Theorem 16. For the second part we observe that

$$f_3(k) = N_3(k) - N_3(k-1).$$

□

5 Volume estimates for $n = 4$

Lemma 4. *The domain $\mathcal{M}_3(p)$ is the collection of 3×3 lower triangular matrices*

$$\begin{pmatrix} x_{11} & & \\ x_{21} & x_{22} & \\ x_{31} & x_{32} & x_{33} \end{pmatrix}$$

with entries in $\mathbb{Z}_p$ such that the following inequalities hold:

[4-1] $v_p(x_{11}) \leq v_p(x_{21}^2 - x_{21}x_{22})$
[4-2] $v_p(x_{11}) \leq v_p(x_{21}(x_{31} - x_{32}))$
[4-3] $v_p(x_{22}) \leq v_p(x_{32}^2 - x_{32}x_{33})$
[4-4] $v_p(x_{11}) + v_p(x_{22}) \leq v_p(x_{22}(x_{31}^2 - x_{31}x_{33}) - x_{21}(x_{32}^2 - x_{32}x_{33}))$.

Proof. We are looking for matrices

$$M = \begin{pmatrix} x_{11} & 0 & 0 \\ x_{21} & x_{22} & 0 \\ x_{31} & x_{32} & x_{33} \end{pmatrix},$$

such that $x_{11}, x_{21}, x_{22}, x_{31}, x_{32}, x_{33} \in \mathbb{Z}_p$ and for $1 \leq i, j \leq 3$, $v_i \circ v_j = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3$, where $\alpha_i \in \mathbb{Z}_p$ and v_i is the i^{th} row of the matrix M.

The condition that $v_2 \circ v_2 = \alpha_1 v_1 + \alpha_2 v_2$ gives the same condition that we had for the case $n = 3$. That is, $v_p(x_{11}) \leq v_p(x_{21}^2 - x_{21}x_{22})$.

We have

$$v_2 \circ v_3 = (x_{21}x_{31}, x_{22}x_{32}, 0) = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3.$$

Clearly $\alpha_3 = 0$. We have $\alpha_2 x_{22} = x_{32}x_{22}$, so $\alpha_2 = x_{32}$. So we have $\alpha_1 x_{11} + x_{32}x_{21} = x_{21}x_{31}$. This implies

$$\alpha_1 = x_{11}^{-1}(x_{21}x_{31} - x_{21}x_{32}).$$

Therefore $v_p(x_{11}) \leq v_p(x_{21}(x_{31} - x_{32}))$.

Next consider

$$v_3 \circ v_3 = (x_{31}^2, x_{32}^2, x_{33}^2) = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3.$$

We must have $\alpha_3 = x_{33}$. So $\alpha_2 x_{22} + x_{33}x_{32} = x_{32}^2$. This implies

$$\alpha_2 = x_{22}^{-1}(x_{32}^2 - x_{32}x_{33}).$$

Therefore $v_p(x_{22}) \leq v_p(x_{32}^2 - x_{32}x_{33})$.

We also have $\alpha_1 x_{11} + x_{22}^{-1}(x_{32}^2 - x_{32}x_{33})x_{21} + x_{33}x_{31} = x_{31}^2$. This implies

$$\begin{aligned} \alpha_1 &= x_{11}^{-1}(x_{31}^2 - x_{31}x_{33} - x_{22}^{-1}x_{21}(x_{32}^2 - x_{32}x_{33})x_{21}) \\ &= x_{11}^{-1}x_{22}^{-1}(x_{22}(x_{31}^2 - x_{31}x_{33}) - x_{21}(x_{32}^2 - x_{32}x_{33})). \end{aligned}$$

So $v_p(x_{11}) + v_p(x_{22}) \leq v_p(x_{22}(x_{31}^2 - x_{31}x_{33}) - x_{21}(x_{32}^2 - x_{32}x_{33}))$.

□

Suppose that $v_p(x_{11}) = k,\ v_p(x_{22}) = l$ and $v_p(x_{33}) = r$. By multiplying by appropriate units, we can suppose that $x_{11} = p^k,\ x_{22} = p^l$ and $x_{33} = p^r$. Note that this does not change the lattice generated by the rows.

Theorem 3. *Suppose that $k, l, r \geq 0$. Then*

$$\mu_p(k; l; r) \leq 8p^{-7k/6}p^{-l/6}. \tag{2}$$

Proof. We have three steps.

Step I. By Proposition 4 the volume of x_{32} satisfying inequality $[4-3]$ is at most $2p^{-l/2}$. By Proposition 4 the volume of x_{21} satisfying inequality $[4-1]$ is at most $2p^{-k/2}$, and for fixed x_{21}, x_{32}, Proposition 8 implies that the volume of x_31 satisfying inequality $[4-4]$ is at most $2p^{-k/2}$. Multiplication gives:

$$\mu_p(k; l; r) \leq 8p^{-k}p^{-l/2}.$$

Step II. By Proposition 5 the volume of x_{21} satisfying inequality $[4-1]$ is at most $2p^{-k+l}$. By Proposition 4 the volume of x_{32} satisfying inequality $[4-3]$ is at most $2p^{-l/2}$. By Proposition 8 the volume of x_{31} satisfying inequality $[4-4]$ is at most $2p^{-k/2}$. Multiplication gives

$$\mu_p(k; l; r) \leq 8p^{-3k/2}p^{l/2}.$$

Step III. We now consider an appropriate average. The idea is that if $\mu \leq A$ and $\mu \leq B$, with $\mu, A, B > 0$, then for all m, n positive integers

$$\mu \leq (A^m B^n)^{\frac{1}{m+n}}.$$

We have

$$\mu_p(k; l; r) \leq 8p^{-k}p^{-l/2}$$

and

$$\mu_p(k; l; r) \leq 8p^{-3k/2}p^{l/2}.$$

We then have

$$\begin{aligned} \mu_p &\leq \left\{ \left(8p^{-k}p^{-l/2}\right)^2 \left(8p^{-3k/2}p^{l/2}\right) \right\}^{1/3} \\ &= 8p^{-7k/6}p^{-l/6}. \end{aligned}$$

□

Remark 2. This is not the best possible bound one can prove. In fact using a more complicated argument similar to the proof of *Step I* of Theorem 9 we can prove a bound of $Cp^{-9k/8}p^{-l/2}$ in *Step I* of the above theorem. This leads to the bound $\mu_p \leq Cp^{-5k/4}p^{-l/2}$ after averaging. This however will not improve the bound in Theorem 6 unless one has an analogue of Theorem 11 for $r = 1$. Such a theorem is easy to prove, but the resulting estimate would still not be good enough to establish Conjecture 1 for $n = 4$. Since [9] contains a proof of Conjecture 1 for $n = 4$, we decided to include only the simplest non-trivial estimate.

Theorem 4. *Let p be odd. If $r = 0$ and $k, l \geq 1$, then*

$$\mu_p(k; l; 0) \leq 48p^{-3k/2-l}.$$

Proof. Proposition 4 implies that inequality $[4-1]$ holds on a set of volume at most $2p^{-\lceil k/2 \rceil}$. Proposition 5 implies that inequality $[4-3]$ holds on a set of x_{32} of volume at most $2p^{-l}$. For fixed x_{21}, x_{32}, Proposition 9 implies that inequality $[4-4]$ holds on a set of x_{31} of volume at most $6p^{-k}$.

We see that our total volume is bounded by $48p^{-k-l-\lceil k/2 \rceil}$. □

Theorem 5. *Let p be odd. If $k = r = 0$, the volume is at most $2p^{-l}$. If $l = r = 0$, then volume is at most $3p^{-2k}$.*

Proof. If $k = r = 0$, then inequality $[4-3]$ and Proposition 4 give the result. Now suppose $l = r = 0$. Then we have

$$v_p(x_{21}) + v_p(x_{21} - 1) \geq k$$

which determines two possibilities for x_{21}:

1. $v_p(x_{21}) \geq k$. In this case inequality $[4-4]$ says

$$v_p(x_{31}) + v_p(x_{31} - 1) \geq k$$

The volume of such x_{31} is $2p^{-k}$. As a result the whole volume is $2p^{-2k}$.

2. $v_p(x_{21}) = 0$ and $v_p(x_{21} - 1) \geq k$. Then inequality $[4-2]$ gives

$$v_p(x_{31} - x_{32}) \geq k$$

and the two dimensional volume of (x_{31}, x_{32}) satisfying this inequality is at most p^{-k}. This way we get p^{-2k}.

Adding up gives the result.

□

6 Convergence for $n = 4$

In this section we prove the following theorem:

Theorem 6. *The expression*

$$\sum_p \sum_{k+l+r \geq 2} p^{2k+l-k\sigma-l\sigma-r\sigma} \mu_p(k; l; r) \tag{3}$$

converges whenever $\sigma > \frac{11}{12}$.

Proof. We write the sum as

$$\sum_{k+l+r \geq 2} 2^{2k+l-k\sigma-l\sigma-r\sigma} \mu_2(k; l; r) + \sum_{p \text{ odd}} \sum_{k+l+r \geq 2} p^{2k+l-k\sigma-l\sigma-r\sigma} \mu_p(k; l; r).$$

By Theorem 3 the first piece is majorized by

$$\sum_{k,l,r \geq 0} 2^{2k+l-k\sigma-l\sigma-r\sigma} 2^{-7k/6} 2^{-l/6}$$

which converges for $\sigma > 5/6$.

We now consider the second piece of the sum. We consider three cases.

Case I. $r \geq 2$. By Theorem 3 the relevant sum is bounded by

$$\sum_{p \text{ odd}} \sum_{r \geq 2} \sum_{k,l \geq 0} p^{2k+l-k\sigma-l\sigma-r\sigma} p^{-7k/6} p^{-l/6} = \sum_{p \text{ odd}} \sum_{r \geq 2} \sum_{k,l \geq 0} p^{(\frac{5}{6}-\sigma)(k+l)-r\sigma}$$

which converges when

$$\sum_{p \text{ odd}} \sum_{r \geq 2} \sum_{k,l \geq 0} p^{(\frac{5}{6}-\sigma)(k+l)-r\sigma}$$

converges. The last sum is equal to

$$\sum_{p \text{ odd}} \sum_{r \geq 2} \sum_{m \geq 0} C_m p^{(\frac{5}{6}-\sigma)m-r\sigma}$$

with C_m the number of solutions (k, l) of $k + l = m$ in non-negative integers. This sum is seen to converge for $\sigma > \frac{5}{6}$.

Case II. $r = 1$. From the previous computation the corresponding sum converges if the following sum converges

$$\sum_{p \text{ odd}} \sum_{m \geq 1} p^{(\frac{5}{6}-\sigma)m-\sigma}.$$

If $\sigma > \frac{5}{6}$, the series converges if the series

$$\sum_{p \text{ odd}} p^{(\frac{5}{6}-\sigma)-\sigma}$$

converges. The latter converges for $\sigma > 11/12$.

Case III. $r = 0$. We write the corresponding sum as

$$\sum_{p \text{ odd}} \sum_{\substack{k+l \geq 2 \\ r=0}} = \sum_{p \text{ odd}} \sum_{\substack{l \geq 2 \\ k=r=0}} + \sum_{p \text{ odd}} \sum_{\substack{k \geq 2 \\ l=r=0}} + \sum_{p \text{ odd}} \sum_{\substack{k,l \geq 1 \\ r=0}}.$$

By Theorem 5 we have

$$\sum_{p \text{ odd}} \sum_{\substack{l \geq 2 \\ k=r=0}} \ll \sum_{p \text{ odd}} \sum_{l \geq 2} p^{-l\sigma}$$

and this is convergent for $\sigma > 1/2$. Again by the same theorem

$$\sum_{p \text{ odd}} \sum_{\substack{k \geq 2 \\ l=r=0}} \ll \sum_{k \geq 2} p^{-k\sigma}$$

which converges for $\sigma > 1/2$. Finally by Theorem 4

$$\sum_{p \text{ odd}} \sum_{\substack{k,l \geq 1 \\ r=0}} \ll \sum_{p \text{ odd}} \sum_{k,l \geq 1} p^{(\frac{1}{2}-\sigma)k-l\sigma}.$$

If $\sigma > \frac{1}{2}$ this last series converges if the series

$$\sum_{p \text{ odd}} p^{(\frac{1}{2}-\sigma)-\sigma}$$

converges. This last series converges for $\sigma > \frac{3}{4}$. □

We have proved the following theorem:

Theorem 7. *There is a polynomial P_4 of degree 5 such that for all $\epsilon > 0$*

$$N_4(B) = BP_4(\log B) + O(B^{\frac{11}{12}+\epsilon})$$

as $B \to \infty$. This gives

$$f_4(k) = O(k^{\frac{11}{12}+\epsilon}).$$

7 Volume estimate for $n = 5$

We will now consider the relevant matrices for $n = 5$ and go through a similar volume computation. We will begin with the set of inequalities defining our region of integration.

Lemma 5. *$\mathcal{M}_4(p)$ is the collection of matrices with entries in $\mathbb{Z}_p$*

$$\begin{pmatrix} x_{11} & & & \\ x_{21} & x_{22} & & \\ x_{31} & x_{32} & x_{33} & \\ x_{41} & x_{42} & x_{43} & x_{44} \end{pmatrix}$$

whose entries satisfy:

$$\begin{aligned}
&\textit{[5-1]} && v_p(x_{11}) \le v_p(x_{21}^2 - x_{21}x_{22}) \\
&\textit{[5-2]} && v_p(x_{11}) \le v_p(x_{21}(x_{31} - x_{32})) \\
&\textit{[5-3]} && v_p(x_{22}) \le v_p(x_{32}^2 - x_{32}x_{33}) \\
&\textit{[5-4]} && v_p(x_{11}) + v_p(x_{22}) \le v_p(x_{22}(x_{31}^2 - x_{31}x_{33}) - x_{21}(x_{32}^2 - x_{32}x_{33})) \\
&\textit{[5-5]} && v_p(x_{11}) \le v_p(x_{21}(x_{41} - x_{42})) \\
&\textit{[5-6]} && v_p(x_{22}) \le v_p(x_{32}(x_{42} - x_{43})) \\
&\textit{[5-7]} && v_p(x_{11}) + v_p(x_{22}) \le v_p(x_{22}x_{31}(x_{41} - x_{43}) - x_{21}x_{32}(x_{42} - x_{43})) \\
&\textit{[5-8]} && v_p(x_{33}) \le v_p(x_{43}^2 - x_{43}x_{44}) \\
&\textit{[5-9]} && v_p(x_{22}) + v_p(x_{33}) \le v_p(x_{33}x_{42}(x_{42} - x_{44}) - x_{32}x_{43}(x_{43} - x_{44})) \\
&\textit{[5-10]} && v_p(x_{11}) + v_p(x_{22}) + v_p(x_{33}) \le v_p(x_{22}x_{33}x_{41}(x_{41} - x_{44}) - x_{22}x_{31}x_{43}(x_{43} - x_{44}) \\
& && -x_{21}x_{33}x_{42}(x_{42} - x_{44}) + x_{21}x_{32}x_{43}(x_{43} - x_{44}).
\end{aligned}$$

The proof of this lemma is very similar to the proof of Lemma 4.

By multiplying by appropriate units, we can suppose that $x_{11} = p^k,\ x_{22} = p^l,\ x_{33} = p^r$ and $x_{44} = p^t$.

We will prove the following.

Theorem 8. *Let p be any prime. Suppose that $k, l, r, t \ge 0$. Then for a constant C which is a polynomial in k we have*

$$\mu_p(k; l; r; t) \le Cp^{-(2+\frac{1}{34})k-(1+\frac{1}{34})l-\frac{r}{17}+\frac{16t}{17}}.$$

Proof. We have several steps:

Step I. Here we show that the volume is bounded by a constant times p^{-2k-l}. The key to our argument will be that once our other variables are fixed, there are several different bounds available to us for the volume of x_{31} such that inequalities $[5-4]$ and $[5-10]$ hold.

Proposition 4 implies that inequality $[5-3]$ holds on a set of x_{32} of volume at most $2p^{-l/2}$.

Suppose that $v_p(x_{43}(x_{43}-x_{44}))=r+z$. Inequality $[5-8]$ implies that $z\geq 0$. This inequality holds on a set of x_{43} of volume at most $2p^{-r/2-z/2}$. Fix some x_{43} satisfying this.

Now for fixed x_{32}, x_{43}, Proposition 8 implies that inequality $[5-9]$ holds on a set of x_{42} of volume at most $2p^{-l/2}$.

We now consider inequality $[5-5]$. For fixed x_{42}, Proposition 7 implies that the total volume of x_{21}, x_{41} such that this inequality holds is at most $(k+1)p^{-k}$.

Finally, we consider x_{31}. Consider inequality $[5-10]$. For fixed $x_{21}, x_{32}, x_{41}, x_{42}, x_{43}$, we can write this as

$$k+l+r\leq v_p(x_{31}x_{22}y-\tau),$$

where $y,\tau\in\mathbb{Z}_p$ with $v_p(y)=r+z$. We see that this holds on a set of x_{31} of volume at most $2p^{-(k-z)}$.

Consider inequality $[5-4]$. By Proposition 8, this holds on a set of x_{31} of volume at most $2p^{-k/2}$.

Using $2p^{-(k-z)}$ as our bound for the volume of x_{31} gives a bound on our total volume of

$$Cp^{-2k-l-(r-z)/2}.$$

This is enough for our result if $r\geq z$. Suppose that this is not the case.

By the proof of Proposition 3.7, we see that the total volume of x_{31} such that

$$v_p(x_{31}(x_{31}-x_{33})-z)\geq k,$$

is at most $6p^{-(k-r)}$ unless $p=2$, $v_p(x_{31})=r-1$ and $v_p(z)=2r-2<k$. If we are not in this exceptional situation the total volume is at most $C'p^{-2k-l-(z/2-r/2)}$. Since $r<z$, this is at most $C'p^{-2k-l}$, completing the proof.

Suppose that we are in the situation where $p=2$, $v_p(x_{31})=r-1$ and $v_p(z)=2r-2<k$.

First suppose that $v_p(x_{31})\neq v_p(x_{32})$. Then $v_p(x_{31}-x_{32})\leq v_p(x_{31})=r-1$. Inequality $[5-2]$ now holds on a set of x_{21} of volume at most $p^{-(k-r)}$. Using this bound for the volume of x_{21}, $2p^{-l/2}$ for the volume of x_{32} and $2p^{-k/2}$ for the volume of x_{31}, gives the total bound

$$Cp^{-2k-l-(z-r)/2},$$

which is at most Cp^{-2k-l} since $z\geq r$.

Now suppose $v_p(x_{32})=v_p(x_{31})=r-1$. Then $v_p(x_{32}(x_{32}-x_{33}))=2r-2$, and we must have $v_p(x_{21})=l$. Now consider inequality $[5-7]$. We write $x_{21}=\alpha p^l$, $x_{31}=\beta p^{r-1}$, and $x_{32}=\gamma p^{r-1}$ for units α,β,γ. Factoring out p^{l+r-1}, the inequality is now

$$v_p(\beta x_{41}-\alpha\gamma x_{42}+(\alpha\gamma-\beta)x_{43})\geq k-r+1.$$

For fixed values of $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, this holds on a set of x_{41} of volume at most $p^{-(k-r)}$. Using $2p^{-k/2}$ as our bound for x_{21} and x_{31}, this gives total bound

$$Cp^{-2k-l-(z-r)/2},$$

which is at most Cp^{-2k-l}, completing *Step I.*

Step II. Here we show that the following three inequalities hold:

$$\mu_p(k;l;r;t) \leq Cp^{-3k/2-3l/2+t} \quad (4)$$

$$\mu_p(k;l;r;t) \leq Cp^{-2k-l-r+3t} \quad (5)$$

$$\mu_p(k;l;r;t) \leq Cp^{-5k/2-l+r+3t}. \quad (6)$$

We proceed as follows. Inequality $[5-1]$ holds on a set x_{21} of volume at most $2p^{-k/2}$ or $2p^{-(k-l)}$. Inequality $[5-3]$ holds on a set x_{32} of volume at most $2p^{-l/2}$ or $2p^{-(l-r)}$. Inequality $[5-8]$ holds on a set of x_{43} of volume at most $2p^{-(r-t)}$.

When $p \neq 2$, we can use Proposition 9 for the remaining three variables (See the proof of Theorem 9 for details). For $p = 2$, some care is required. By Proposition 8 we always have the following. For any fixed x_{21} and x_{32} inequality $[5-4]$ holds on a set of x_{31} of volume at most $2p^{-k/2}$. For any fixed x_{32}, x_{43} inequality $[5-9]$ holds on a set of x_{42} of volume at most $2p^{-l/2}$. For any fixed $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$ inequality $[5-10]$ holds on a set of x_{41} of volume at most $2p^{-k/2}$.

Inequality (4) now follows from taking $2p^{-k/2}$ for the volume of x_{21}, x_{31}, x_{41}, taking $2p^{-(l-r)}$ for the volume of x_{32}, taking $2p^{-l/2}$ for the volume of x_{42}, and taking $2p^{-(r-t)}$ for the volume of x_{43}.

For inequality (5) we take $2p^{-k/2}$ as our bound for the volume of x_{21} and x_{31}, $2p^{-l/2}$ as the bound for x_{32} and x_{42}, and $2p^{-(r-t)}$ as the bound for the volume of x_{43}. We must now show that when all other variables are fixed, the total volume of x_{41} satisfying our inequalities is at most $Cp^{-(k-2t)}$. When we are not in the special case where we cannot apply Proposition 9, we have that the volume of x_{41} satisfying inequality $[5-10]$ is at most $6p^{-(k-t)}$, completing this case.

We can write inequality $[5-10]$ as

$$v_p(x_{11}) + v_p(x_{22}) + v_p(x_{33}) \leq v_p(x_{22}x_{33}x_{41}(x_{41} - x_{44}) - (x_{22}x_{31}x_{43}(x_{43} - x_{44}) \\ +x_{21}(x_{33}x_{42}(x_{42} - x_{44}) - x_{32}x_{43}(x_{43} - x_{44}))).$$

Inequality $[5-8]$ implies that we can write $x_{43}(x_{43} - x_{44}) = p^r\alpha$, with $\alpha \in \mathbb{Z}_p$. Inequality $[5-9]$ implies that we can write

$$x_{33}x_{42}(x_{42} - x_{44}) - x_{32}x_{43}(x_{43} - x_{44}) = p^{l+r}\beta,$$

with $\beta \in \mathbb{Z}_p$.

Our inequality is now

$$k \leq v_p(x_{41}(x_{41} - x_{44}) - (x_{31}\alpha + x_{21}\beta).$$

We can apply Proposition 9, giving our bound, unless $v_p(x_{41}) = t-1$ and $v_p(x_{31}\alpha + x_{21}\beta) = 2t-2$.

First suppose that $v_p(x_{21}) \leq 2t$. Then for fixed x_{21}, x_{42}, inequality $[5-5]$ holds on a set of x_{41} of volume at most $p^{-(k-2t)}$, which completes this case. Now suppose that $v_p(x_{31}) \leq 2t$. Proposition 3 now implies that for fixed $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, inequality $[5-7]$ holds on a set of x_{41} of volume at most $p^{-(k-v_p(x_{31}))} \leq p^{-(k-2t)}$. This is enough for our bound, so we suppose that $v_p(x_{21}) \geq 2t$ and $v_p(x_{31}) \geq 2t$. This implies that $v_p(x_{31}\alpha + x_{21}\beta) \geq 2t > 2t-2$, so we can apply Proposition 9, completing this case.

Inequality (6) will be proved in a few steps. First we suppose that we are in the case where we can apply Proposition 9 to inequality $[5-4]$ and conclude that the volume of x_{31} satisfying this inequality is at most $6p^{-(k-r)}$. As above, we see that either one of x_{21}, x_{31} has valuation at most $2t$, giving a bound of $p^{-(k-2t)}$, or both have valuation at least $2t$, in which case we can apply Proposition 9 and conclude that the total volume of x_{41} is at most $6p^{-(k-t)}$. Using $2p^{-k/2}$ as our bound for x_{21}, $2p^{-l/2}$ as our bound for x_{32} and x_{42}, and $2p^{-(r-t)}$ as our bound for x_{43}, we get total volume

$$Cp^{-5k/2-l+3t},$$

completing this case.

Now suppose that we are in the case where we cannot apply Proposition 9 to inequality $[5-4]$. Then $v_p(x_{31}) = r-1$. We now consider two subcases. First suppose that $v_p(x_{31}) \neq v_p(x_{32})$. Then inequality $[5-2]$ implies that $v_p(x_{21}) \geq k - v_p(x_{31}) > k-r$, which holds on a set of x_{21} of volume at most $p^{-(k-r)}$. We use $2p^{-k/2}$ as the bound for the volume of x_{31} satisfying inequality $[5-4]$.

Now using the same argument given above, the volume of x_{41} satisfying these inequalities is at most $6p^{-(k-2t)}$. Combining these estimates gives total volume bounded by

$$Cp^{-5k/2-l+3t},$$

completing this case.

Finally, suppose that $v_p(x_{31}) = v_p(x_{32}) = r-1$. Now for fixed x_{32}, x_{43}, the total volume of x_{42} satisfying inequality $[5-6]$ is at most $p^{-(l-r)}$. We use $2p^{-(k-l)}$ as the bound on the volume of x_{21} satisfying inequality $[5-1]$, $2p^{-k/2}$ as the bound on the volume of x_{31}, $2p^{-(r-l)}$ as our bound on the volume of x_{32}, and $2p^{-(r-t)}$ as the bound on the volume of x_{43}. Using the same argument given above, we can use $6p^{-(k-2t)}$ as our bound on the volume of x_{41}. This gives total bound

$$Cp^{-5k/2-l+r+3t},$$

completing *Step II.*

Step III. Here we consider an appropriate average of the previous inequalities to prove the theorem. As constants play no role we ignore them. So far we have

$$\mu_p \leq p^{-2k-l},$$

$$\mu_p \leq p^{-3k/2-3l/2+t}$$

$$\mu_p \leq p^{-2k-l-r+3t}$$

and

$$\mu_p \leq p^{-5k/2-l+r+3t}.$$

This means for all $n \geq 1$

$$\begin{aligned}\mu_p \leq & \left\{ \left(p^{-3k/2-3l/2+t}\right)\left(p^{-2k-l-r+3t}\right)^3 \left(p^{-5k/2-l+r+3t}\right)^2 \left(p^{-2k-l}\right)^n \right\}^{1/n+6} \\ = & p^{-(2+\frac{1}{2(n+6)})k-(1+\frac{1}{2(n+6)})l-\frac{r}{n+6}+\frac{16t}{n+6}}.\end{aligned}$$

Setting $n = 11$ gives the result. □

We now state several results for odd primes p.

Theorem 9. *Let p be odd. Suppose that $k, l, r, t \geq 0$. Then for a constant C which is a polynomial in k we have*

$$\mu_p(k;l;r;t) \leq Cp^{-(2+\frac{1}{20})k-(1+\frac{1}{20})l-\frac{r}{20}+\frac{9t}{20}}.$$

Proof. We have several steps:

Step I. Here we show that the volume is bounded by a constant times p^{-2k-l}. The key to our argument will be that once our other variables are fixed, there are several different bounds available to us for the volume of x_{31} such that inequalities $[5-4]$ and $[5-10]$ hold.

Proposition 4 implies that inequality $[5-3]$ holds on a set of x_{32} of volume at most $2p^{-l/2}$.

Suppose that $v_p(x_{43}(x_{43}-x_{44})) = r+z$. Inequality $[5-8]$ implies that $z \geq 0$. This inequality holds on a set of x_{43} of volume at most $2p^{-r/2-z/2}$. Fix some x_{43} satisfying this.

Now fox fixed x_{32}, x_{43}, Proposition 8 implies that inequality $[5-9]$ holds on a set of x_{42} of volume at most $2p^{-l/2}$.

We now consider inequality $[5-5]$. For fixed x_{42}, Proposition 7 implies that the total volume of x_{21}, x_{41} such that this inequality holds is at most $(k+1)p^{-k}$.

Finally, we consider x_{31}. For fixed x_{21}, x_{32}, we see that inequality $[5-4]$ holds on a set of x_{31} of volume at most $6p^{-(k-r)}$.

Consider inequality $[5-10]$. For fixed $x_{21}, x_{32}, x_{41}, x_{42}, x_{43}$, we can write this as

$$k+l+r \leq v_p(x_{31}x_{22}y-\tau),$$

where $y, \tau \in \mathbb{Z}_p$ with $v_p(y) = r+z$. We see that this holds on a set of x_{31} of volume at most $2p^{-(k-z)}$.

We now have two bounds on the total volume of the variables satisfying our inequalities: one coming from using $6p^{-(k-r)}$ as an upper bound for the volume of x_{31}, and the other from using $2p^{-(k-z)}$. The total volume is at most

$$\min\{C'p^{-(2k-l-(r/2-z/2)}, \ C'p^{-2k-l-(z/2-r/2)}\}.$$

It is clear that since either $r \leq z$ or $z \leq r$, at least one of these terms is at most Cp^{-2k-l}, completing the proof.

Step II. Here we show that the following three inequalities hold:

$$\mu_p(k;l;r;t) \leq Cp^{-2k-3l/2-r+3t},$$

$$\mu_p(k;l;r;t) \leq Cp^{-3k-l+r+3t},$$

and

$$\mu_p(k;l;r;t) \leq Cp^{-5k/2-3l/2+3t}. \tag{7}$$

We will use (7) in the proof of Theorem 11. We proceed as follows. Inequality $[5-1]$ holds on a set x_{21} of volume at most $2p^{-k/2}$ or $2p^{-(k-l)}$. Inequality $[5-3]$ holds on a set x_{32} of volume at most $2p^{-l/2}$ or $2p^{-(l-r)}$. Inequality $[5-8]$ holds on a set of x_{43} of volume at most $2p^{-(r-t)}$. For any fixed x_{21} and x_{32} inequality $[5-4]$ holds on a set of x_{31} of volume at most $2p^{-k/2}$ or $6p^{-(k-r)}$. For any fixed x_{32}, x_{43} inequality $[5-9]$ holds on a set of x_{42} of volume at most $6p^{-(l-t)}$. For any fixed $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$ inequality $[5-10]$ holds on a set of x_{41} of volume at most $6p^{-(k-t)}$. Hence the total volume is bounded by

$$Cp^{-(k-t)}.p^{-(l-t)}.p^{-(r-t)}.p^{-k/2}.p^{-l/2}.p^{-k/2},$$

by

$$Cp^{-(k-t)}.p^{-(l-t)}.p^{-(r-t)}.p^{-(k-l)}.p^{-(l-r)}.p^{-(k-r)},$$

and by

$$Cp^{-(k-t)}.p^{-(l-t)}.p^{-(r-t)}.p^{-k/2}.p^{-l/2}.p^{-(k-r)}.$$

Simplification gives the result.

Step III. Here we consider an appropriate average of the previous inequalities to prove the theorem. As constants play no role we ignore them. So far we have

$$\mu_p \leq p^{-2k-l},$$

$$\mu_p \leq p^{-2k-3l/2-r+3t}$$

and

$$\mu_p \leq p^{-3k-l+r+3t}.$$

This means for all $n \geq 1$

$$\begin{aligned}\mu_p \leq & \left\{ \left(p^{-2k-3l/2-r+3t}\right)^2 \left(p^{-3k-l+r+3t}\right) \left(p^{-2k-l}\right)^n \right\}^{1/n+3} \\ = & p^{-(2+\frac{1}{n+3})k-(1+\frac{1}{n+3})l-\frac{r}{n+3}+\frac{9t}{n+3}}.\end{aligned}$$

Setting $n = 17$ gives the result. $\square$

Theorem 10. *Let p be odd. If $v_p(x_{44}) = t = 0$, then for any $k+l+r \geq 2$, the volume of the above domain is bounded by*

$$Cp^{-(2+\frac{1}{7})k-(1+\frac{1}{7})l-\frac{r}{7}-\frac{8}{7}}$$

for some constant $C > 0$.

Proof. We have two basic steps:

Step I. Here we will show that $\mu_p \leq Cp^{-2k-l-2}$ whenever $k+l+r \geq 2$. We first note that Proposition 5 implies that inequality $[5-8]$ holds on a set of x_{43} of volume at most $2p^{-(r-t)} = 2p^{-r}$. Inequality $[5-3]$ holds on a set of x_{32} of volume at most $2p^{-\lceil l/2 \rceil}$.

Proposition 4 implies that inequality $[5-1]$ holds on a set of x_{21} of volume at most $2p^{-\lceil k/2 \rceil}$. For fixed x_{21}, x_{32}, Proposition 8 implies that the total volume of x_{31} satisfying inequality $[5-4]$ is at most $2p^{-\lceil k/2 \rceil}$.

For fixed $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, inequality $[5-10]$ can be written as

$$k+l+r \leq v_p(x_{22}x_{33}x_{41}(x_{41}-x_{44})-z),$$

for some $z \in \mathbb{Z}_p$. Proposition 9 implies that this holds on a set of x_{41} of volume at most $6p^{-k}$.

Therefore, our total volume is at most

$$Cp^{-k-2\lceil k/2 \rceil - l - \lceil l/2 \rceil - r},$$

for some $C > 0$. If $r + \lceil l/2 \rceil \geq 2$, we are done. Therefore, suppose $r = 0$ and $l \in \{0,1,2\}$ or $r = 1$ and $l = 0$.

First suppose $r = 0$. Then Proposition 5 implies that inequality $[5-3]$ holds on a set of x_{32} of volume at most $2p^{-l}$. For fixed x_{21}, x_{32}, Proposition 9 implies that inequality $[5-4]$ holds on a set of x_{31} of volume at most $6p^{-k}$. Using the above bounds for x_{42} and x_{41}, our total volume is now bounded by

$$Cp^{-2k-\lceil k/2 \rceil - 2l}.$$

Since $k+l \geq 2$, we have $\lceil k/2 \rceil + l \geq 2$ unless $l = 0$ and $k = 2$. In this case, we use $2p^{-k}$ as a bound for the volume of x_{21} satisfying inequality $[5-1]$, which completes this case.

Now suppose $r = 1$ and $l = 0$. Proposition 5 implies that the volume of x_{21} satisfying inequality $[5-1]$ is at most $2p^{-k}$. For fixed x_{21}, x_{32}, Proposition 8 implies that the total volume of x_{31} satisfying inequality $[5-4]$ is at most $2p^{-\lceil k/2 \rceil}$. We use the same bounds for the volume of x_{43} and x_{41}. Our total volume is now bounded by

$$Cp^{-2k-\lceil k/2 \rceil - 1}.$$

Since $k+l+r \geq 2$, we have $k \geq 1$ and our bound is at most Cp^{-2k-2}, completing the proof.

Step II. This step is very similar to the last step of the proof of Theorem 9. We have by the above and the second step of the proof of Theorem 9

$$\mu_p \leq p^{-2k-l-2},$$

$$\mu_p \leq p^{-2k-3l/2-r}$$

and

$$\mu_p \leq p^{-3k-l+r}.$$

This means for all $n \geq 1$

$$\begin{aligned}\mu_p \leq & \left\{ \left(p^{-2k-3l/2-r}\right)^2 \left(p^{-3k-l+r}\right) \left(p^{-2k-l-2}\right)^n \right\}^{1/n+3} \\ = & p^{-(2+\frac{1}{n+3})k-(1+\frac{1}{n+3})l-\frac{r}{n+3}-\frac{2n}{n+3}}.\end{aligned}$$

Setting $n = 4$ gives the result.

□

We can similarly handle the case where $t = 1$.

Theorem 11. *Let p be odd. If $v_p(x_{44}) = t = 1$, then for any $k+l+r \geq 1$, the volume of the above domain is bounded by*

$$Cp^{-(2+\frac{1}{18})k-(1+\frac{1}{9})l-\frac{r}{9}-\frac{1}{9}},$$

for some constant $C > 0$.

Proof. We have two main steps:

Step I. Here we will show that the volume is bounded by

$$Cp^{-2k-l-1}.$$

We recall that inequality $[5-1]$ holds on a set of x_{21} of volume at most the minimum of $2p^{-\lceil k/2 \rceil}$, and $2p^{-(k-l)}$. Similarly, inequality $[5-3]$ holds on set x_{32} of volume at most the minimum of $2p^{-\lceil l/2 \rceil}$, and $2p^{-(l-r)}$. We also have that inequality $[5-8]$ holds on a set of x_{43} of volume at most the minimum of $2p^{-\lceil r/2 \rceil}$, and $2p^{-(r-t)} = 2p^{-(r-1)}$.

For any fixed values of x_{21}, x_{32}, we see that inequality $[5-4]$ holds on a set of x_{31} of volume at most the maximum of $2p^{-\lceil k/2 \rceil}$, and $6p^{-(k-r)}$. For any fixed values of x_{32}, x_{43}, we see that inequality $[5-9]$ holds on a set of x_{42} of volume at most the maximum of $2p^{-\lceil l/2 \rceil}$, and $6p^{-(l-1)}$. For any fixed values of $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, we can write inequality $[5-10]$ as $k \leq v_p(x_{41}(x_{41}-x_{44})-z)$, for some $z \in \mathbb{Z}_p$. This holds on a set of x_{41} of volume at most the maximum of $2p^{-\lceil k/2 \rceil}$, and $6p^{-(k-1)}$.

We now combine these inequalities to get bounds on the total volume satisfying inequalities $[5-1]$ through $[5-10]$. Note that if $k-l \geq \lceil k/2 \rceil$ and $l-r \geq \lceil l/2 \rceil$, then $k-r \geq \lceil k/2 \rceil$. By using $2p^{-\lceil k/2 \rceil}$ as the bound for the volume of x_{21} and x_{31}, and $2p^{-(l-r)}$ as the bound for x_{32}, we see that our total volume is bounded by

$$Cp^{-k-2l-2\lceil k/2 \rceil+3}.$$

Therefore, we are done if $l \geq 4$, or if $l \geq 3$ and k is odd. Suppose that this is not the case.

Suppose that $l \leq 3$. Using $2p^{-\lceil l/2 \rceil}$ instead of $2p^{-(l-r)}$ as our bound for the volume of x_{32}, our total bound is now

$$Cp^{-k-2\lceil k/2 \rceil-l-\lceil l/2 \rceil-r+3}.$$

Therefore, we are done if $\lceil l/2 \rceil + r \geq 4$, or $\lceil l/2 \rceil + r \geq 3$ and k is odd. Suppose that these conditions do not hold.

First suppose that $l = 3$. Then $r \leq 1$. We can use $2p^{-\lceil r/2 \rceil}$ as a bound for the total volume of x_{43} satisfying inequality $[5-8]$ instead of $2p^{-(r-1)}$. We use $2p^{-(l-r)}$ as our bound for the volume of x_{32} satisfying inequality $[5-3]$. We see that our total volume is bounded by

$$Cp^{-k-2\lceil k/2 \rceil-3-3+r-\lceil r/2 \rceil+2} = Cp^{-k-2\lceil k/2 \rceil-4+r-\lceil r/2 \rceil}.$$

Since $r \leq 1$, this is at most $Cp^{-2k-l-1}$, completing this case.

Now suppose that $l \leq 2$. For fixed x_{32}, x_{43}, Proposition 8 implies that the total volume of x_{42} satisfying inequality $[5-9]$ is at most $2p^{-\lceil l/2 \rceil}$. We use this bound instead of $6p^{-(l-1)}$. Our total volume is now bounded by

$$Cp^{-k-2\lceil k/2 \rceil-2\lceil l/2 \rceil-r+2},$$

and we are done unless $r \leq 2$. In this case $\lceil r/2 \rceil \geq r-1$, so we use $2p^{-\lceil r/2 \rceil}$ as our bound for the volume of x_{43} satisfying inequality $[5-8]$. Now our bound is

$$Cp^{-k-2\lceil k/2 \rceil-2\lceil l/2 \rceil-\lceil r/2 \rceil+1}.$$

First suppose $r = 2$. Then if l is odd or k is odd, we are done. If $l = 0$, then we can use $2p^{-k}$ as our bound for the volume of x_{21} satisfying inequality $[5-1]$, giving

$$Cp^{-2k-\lceil k/2\rceil},$$

as our bound. Therefore, we are done unless $k = 0$. In this case, $k = l = 0$, we have that the total volume is at most the total volume of x_{43} satisfying inequality $[5-9]$, which is at most $2p^{-1}$, which completes this case.

Now suppose $r = l = 2$. This is the most difficult case to consider. If k is odd then $2\lceil k/2\rceil = k+1$, and we are done. If $k \geq 6$, then we can use $2p^{-(k-l)}$ as our bound for x_{21}, which is enough to complete this case. If $k = 0$, then we use 1 as our bound for x_{41} instead of $6p^{-(k-1)}$, and our total bound is Cp^{-l-1}, completing this case. We now must consider $k = 2$ and $k = 4$.

First suppose $k = 2$. We need a bound of Cp^{-7}. Using $2p^{-\lceil k/2\rceil}$ as our bound for x_{21}, x_{31}, x_{41}, $2p^{-\lceil l/2\rceil}$ as our bound for x_{32} and x_{42}, and $2p^{-\lceil r/2\rceil}$ as our bound for x_{43}, we get a bound of Cp^{-6}. Since $l = k = 2$ inequality $[5-1]$ becomes $2v_p(x_{21}) \geq 2$ and inequality $[5-3]$ becomes $2v_p(x_{32}) \geq 2$. If either of these variables has valuation greater than 1, then we will have the upper bound that we need. Therefore, we need only consider the case where $v_p(x_{21}) = v_p(x_{32}) = 1$. Inequality $[5-2]$ now implies that $v_p(x_{31} - x_{32}) \geq 1$. Therefore, $v_p(x_{31}) \geq 1$, and we note that if $v_p(x_{32}) \geq 2$, we will have our bound. Therefore we suppose that $v_p(x_{31}) = 1$. Finally, we consider inequality $[5-4]$. We have $v_p(x_{22}(x_{31}^2 - x_{31}x_{33})) = 4 = k + l$, but $v_p(x_{21}(x_{32}^2 - x_{32}x_{33})) = 3 < k + l$, so this case cannot occur.

When $k = 4$ we will argue similarly. We need a bound of Cp^{-11}. Using $2p^{-\lceil k/2\rceil}$ as our bound for x_{21} and x_{31}, $6p^{-(k-1)}$ as our bound for x_{41}, $2p^{-\lceil l/2\rceil}$ as our bound for x_{32} and x_{42}, and $2p^{-\lceil r/2\rceil}$ as our bound for x_{43}, we get a bound of Cp^{-10}. Since $l = r = 2$ inequality $[5-8]$ becomes $2v_p(x_{43}) \geq 2$ and inequality $[5-3]$ becomes $2v_p(x_{32}) \geq 2$. If either of these variables has valuation greater than 1, then we will have the bound that we need. Therefore, we need only consider the case where $v_p(x_{43}) = v_p(x_{32}) = 1$. Inequality $[5-6]$ now implies that $v_p(x_{42} - x_{43}) \geq 1$. Therefore, $v_p(x_{42}) \geq 1$, and we note that if $v_p(x_{42}) \geq 2$, we will have our bound. Therefore we suppose that $v_p(x_{42}) = 1$. Finally, we consider inequality $[5-9]$. We have $v_p(x_{33}(x_{42}^2 - x_{42}x_{43})) = 4 = l + r$, but $v_p(x_{32}(x_{43}^2 - x_{43}x_{44})) = 3 < l + r$, so this case cannot occur.

Next suppose $l \leq 2$ and $r = 1$. We have the bound

$$Cp^{-k-2\lceil k/2\rceil-2\lceil l/2\rceil}.$$

If $l = 1$, we are done. Suppose $l = 2$. Then we can use $2p^{-l}$ as our bound for the volume of x_{32} satisfying inequality $[5-3]$, and we are done. If $l = 0$, then we can use $2p^{-k}$ as the bound for x_{21} satisfying inequality $[5-1]$, and our bound is

$$Cp^{-2k-\lceil k/2\rceil},$$

which completes this case unless $k = 0$. If $k = l = 0$ and $r = t = 1$, then our total volume is at most the volume of x_{43} satisfying inequality $[5-8]$, which is $2p^{-1}$, and we are done.

Finally, suppose $r = 0$ and $l \leq 2$. We can use $2p^{-l}$ as our bound for the volume of x_{32} satisfying inequality $[5-3]$, and for fixed x_{21}, x_{32}, we use $6p^{-k}$ as our bound for the volume of x_{31} satisfying inequality $[5-4]$. We also use $2p^{-\lceil k/2\rceil}$ as our bound for the volume of x_{41} satisfying inequality $[5-10]$. Our total volume is now bounded by

$$Cp^{-2k-\lceil k/2\rceil-l-\lceil l/2\rceil}.$$

Since $k + l + r \geq 1$, we are done.

Step II. Again we do an averaging. We have the inequalities

$$\mu_p \leq p^{-2k-l-1},$$

$$\mu_p \leq p^{-2k-3l/2-r+3}$$

and

$$\mu_p \leq p^{-5k/2-3l/2+3t}.$$

The last two inequalities are from *Step II* of the proof of Theorem 9 for $t = 1$. This means for all $n \geq 1$

$$\begin{aligned}\mu_p \leq & \left\{ \left(p^{-2k-3l/2-r+3}\right)\left(p^{-5k/2-3l/2+3}\right)\left(p^{-2k-l-1}\right)^n \right\}^{1/n+2} \\ = & p^{-(2+\frac{1}{2(n+2)})k-(1+\frac{1}{n+2})l-\frac{r}{n+2}+\frac{6-n}{n+2}}.\end{aligned}$$

We set $n = 7$ to get the result. □

Remark 3. The case by case analysis of the small values of parameters in the proofs of Theorems 10 and 11 can be avoided if instead one uses the results of [9] for $f_n(p^k)$ for small k. In [9] these values are worked out for k up to 5. This is not sufficient for our purposes, but computing the missing data is not difficult using the results of Liu. Here we chose instead to present the above elementary treatment to make the argument self-contained.

8 Convergence for $n = 5$

In this section we prove the following theorem:

Theorem 12. *If $\sigma > \frac{33}{34}$ the expression*

$$\sum_p \sum_{k+l+r+t\geq 2} p^{3k+2l+r-k\sigma-l\sigma-r\sigma-t\sigma}\mu_p(k;l;r;t)$$

converges.

Proof. In our analysis we will ignore all constants as they will have no bearing on convergence. We write

$$\sum_p = \sum_{k+l+r+t\geq 2} 2^{3k+2l+r-k\sigma-l\sigma-r\sigma-t\sigma}\mu_2(k;l;r;t) + \sum_{p \text{ odd}} \sum_{k+l+r+t\geq 2} p^{3k+2l+r-k\sigma-l\sigma-r\sigma-t\sigma}\mu_p(k;l;r;t).$$

If we use Theorem 8 we see very easily that the first piece converges for $\sigma > \frac{33}{34}$. So we concentrate on the sum corresponding to the odd primes. We will consider three cases:

I. $t \geq 2$. Then by Theorem 9 the series is convergent if the following series converges

$$\sum_p \sum_{k,l,r\geq 0} \sum_{t\geq 2} p^{(k+l+r)(1-\frac{1}{20}-\sigma)} p^{\frac{9t}{20}-t\sigma} = \sum_p \sum_{m=0}^{\infty} C_m p^{m(1-\frac{1}{20}-\sigma)} \frac{p^{2(\frac{9}{20}-\sigma)}}{1-p^{\frac{9}{20}-\sigma}}$$

provided that $\sigma > \frac{9}{20}$. Here C_m is the number of solutions of $k+l+r = m$ in non-negative integers. If $\sigma > \frac{19}{20}$ this last series converges.

II. $t = 1$. Then by Theorem 11 the series converges if

$$\sum_p \sum_{k+l+r\geq 1} p^{k(1-\frac{1}{18}-\sigma)} p^{(l+r)(1-\frac{1}{9}-\sigma)} p^{-\sigma-\frac{1}{9}}$$

converges. This last series converges for $\sigma > \frac{17}{18}$.

III. $t = 0$. By Theorem 10 the series converges if

$$\sum_p \sum_{k+l+r\geq 2} p^{(k+l+r)(1-\frac{1}{7}-\sigma)} p^{-\frac{8}{7}} = \sum_p \sum_{m=2}^{\infty} C_m p^{m(1-\frac{1}{7}-\sigma)} p^{-\frac{8}{7}}.$$

This series converges if $\sigma > \frac{6}{7}$. □

Theorem 13. *There is a polynomial P_5 of degree 9 such that for all $\epsilon > 0$*

$$N_5(B) = BP_5(\log B) + O(B^{\frac{33}{34}+\epsilon})$$

as $B \to \infty$. Furthermore,

$$f_5(k) = O(k^{\frac{33}{34}+\epsilon}).$$

Remark 4. Using Theorem 8 for odd primes instead of Theorem 9 in the proof of Theorem 12 would have produced a weaker error term.

9 General n

Here we prove Main Theorem 2. The essential ingredient is the following lemma:

Lemma 6. *Suppose $n \geq 6$. Then there is a constant C which is a polynomial in $k_1, \ldots, k_4$, such that*

$$\mu_p(k_1; \ldots; k_n) \leq C p^{-A_n(p) - \sum_{j=5}^{n} (n-j) \left\lceil \frac{k_j}{2} \right\rceil}$$

with

$$A_n(p) = \left(\frac{n}{2} + \frac{1}{20}\right) k_1 + \left(\frac{n-2}{2} + \frac{1}{20}\right) k_2 + \left(\frac{n-4}{2} + \frac{1}{20}\right) k_3 + \left(\frac{n-4}{2} - \frac{9}{20}\right) k_4,$$

for p odd, and

$$A_n(p) = \left(\frac{n}{2} + \frac{1}{34}\right) k_1 + \left(\frac{n-2}{2} + \frac{1}{34}\right) k_2 + \left(\frac{n-4}{2} + \frac{1}{17}\right) k_3 + \left(\frac{n-4}{2} - \frac{16}{17}\right) k_4,$$

for $p = 2$.

Proof. The proof is by induction on n. The lemma will follow from Theorems 8 and 9 if we show that

$$\mu_p(k_1; \ldots; k_n) \leq 2^{n-1} p^{-\sum_{j=1}^{n-1} \left\lceil \frac{k_j}{2} \right\rceil} \mu_p(k_1; \ldots; k_{n-1}). \tag{8}$$

In order to see this inequality we observe that if

$$M = \begin{pmatrix} p^{k_1} & 0 & \ldots & 0 \\ x_{21} & p^{k_2} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_{n1} & \ldots & \ldots & p^{k_n} \end{pmatrix} \in \mathcal{M}_n(p; k_1, \ldots, k_n)$$

then the matrix obtained by removing the last row

$$M' = \begin{pmatrix} p^{k_1} & 0 & \dots & 0 \\ x_{21} & p^{k_2} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_{n-1\,1} & \dots & \dots & p^{k_{n-1}} \end{pmatrix} \in \mathcal{M}_{n-1}(p; k_1, \dots, k_{n-1}).$$

The inequality (8) will follow if we show that the fibers of the map $M \mapsto M'$ have volume bounded by

$$2^{n-1} p^{-\sum_{j=1}^{n-1} \left\lceil \frac{k_j}{2} \right\rceil}.$$

As usual we set

$$v_j = (x_{j1}, \dots, x_{jj}, 0, \dots, 0).$$

Suppose $v_1, \dots, v_{n-1}$ are the rows of M'. We now bound the volume of the set of vectors v_n with $x_{nn} = p^{k_n}$ such that

$$v_n \circ v_n = c_1 v_1 + \dots + c_n v_n$$

with $c_i \in \mathbb{Z}_p$. It is clear that $c_n = x_{nn}$. We then see that for $1 \leq j \leq n-1$

$$x_{nj}^2 - x_{nn} x_{nj} = c_j x_{jj} + \sum_{k=j+1}^{n-1} c_k x_{kj}.$$

If c_k, x_{kj} are given for $j+1 \leq k \leq n$, then that such a c_j exists is equivalent to

$$v_p \left(x_{nj}^2 - x_{nn} x_{nj} - \sum_{k=j+1}^{n-1} c_k x_{kj} \right) \geq k_j.$$

Proposition 8 implies that the volume of x_{nj} is bounded by $2p^{-\lceil k_j/2 \rceil}$. Induction will give the result. □

We can now present the proof of the Main Theorem 2.

Proof. For convenience we will prove the theorem for $\mathbb{Z}^{n+1}$. We will show that the abscissa of convergence of the counting zeta function is less than or equal to $\frac{n-1}{2} - \frac{1}{20}$. Then as the counting zeta function is an Euler product of cone integrals, the theorem follows from Theorem 1.5 of [5]. We use the lemma to show that the Euler product

$$\prod_p \sum_{k_1, \dots k_n \geq 0} p^{\sum_{j=1}^n (n-j) k_j} p^{-\sigma \sum_{j=1}^n k_j} \mu_p(k_1; \dots; k_n)$$

converges for $\sigma > \frac{n}{2} - \frac{1}{2} - \frac{1}{20}$. It is not hard to see using Lemma 6 that the factor corresponding to $p = 2$ converges in the desired domain. Then we need to show the convergence of the series

$$\begin{aligned} &\sum_{p \text{ odd}} \sum_{k_1 + \dots + k_n \geq 1} p^{\sum_{j=1}^n (n-j) k_j} p^{-\sigma \sum_{j=1}^n k_j} \mu_p(k_1; \dots; k_n) \\ &= \sum_{p \text{ odd}} \sum_{k_1 + \dots + k_n = 1} + \sum_{p} \sum_{k_1 + \dots + k_n \geq 2}. \end{aligned}$$

By Lemma 1

$$\sum_{k_1+\cdots+k_n=1} p^{\sum_{j=1}^n (n-j)k_j} p^{-\sigma\sum_{j=1}^n k_j} \mu_p(k_1;\ldots;k_n) = \binom{n+1}{2} p^{-\sigma}.$$

The sum $\sum_p \binom{n+1}{2} p^{-\sigma}$ converges for $\sigma > 1$. Now we concentrate on the second sum. From here on $\sum_p$ means $\sum_{p \text{ odd}}$. By Lemma 6

$$\begin{aligned}\sum_p \sum_{k_1+\cdots+k_n\geq 2} &\ll \sum_p \sum_{k_1+\cdots+k_n\geq 2} p^{\sum_{j=1}^n (n-j)k_j} p^{-\sigma\sum_{j=1}^n k_j} p^{-A_n - \sum_{j=5}^n (n-j)\left\lceil \frac{k_j}{2}\right\rceil} \\ &\leq \sum_p \sum_{k_1+\cdots+k_n\geq 2} p^{B_n + \frac{1}{2}\sum_{j=5}^n (n-j)k_j} p^{-\sigma\sum_{j=1}^n k_j}\end{aligned}$$

where

$$B_n = \left(\frac{n}{2} - 1 - \frac{1}{20}\right)(k_1+k_2+k_3) + \left(\frac{n}{2} - 2 + \frac{9}{20}\right) k_4.$$

Our series is now bounded by

$$\begin{aligned}&\sum_p \sum_{k_1+\cdots+k_n\geq 2} p^{(\frac{n}{2}-1-\frac{1}{20}-\sigma)\sum_{j=1}^{n-1} k_j} p^{-\sigma k_n} \\ &= \sum_p \sum_{m+k_n\geq 2} C_n(m) p^{(\frac{n}{2}-1-\frac{1}{20}-\sigma)m} p^{-\sigma k_n}\end{aligned}$$

where $C_n(m)$ is the number of solutions of $\sum_{j=1}^{n-1} k_j = m$ for $m \geq 0$. Since $C_n(m)$ is a polynomial in m, this series converges if and only if the series

$$\sum_p \sum_{m+k_n\geq 2} p^{(\frac{n}{2}-1-\frac{1}{20}-\sigma)m} p^{-\sigma k_n}$$

converges. The subseries consisting of $m = 0, k_n \geq 2$ converges if $\sigma > \frac{1}{2}$. If $k_n = 0$ and $m \geq 2$ the series converges provided that $\sigma > \frac{n-1}{2} - \frac{1}{20}$. If $k_n = 1, m = 1$, the series converges if $\sigma > \frac{n}{4} - \frac{1}{40}$. □

10 Tauberian theorems

First we state a simple Tauberian theorem.

Theorem 14. *Suppose we have a Dirichlet series*

$$Z(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \tag{9}$$

which is analytic in some half plane $\Re s > a$, and in that half plane is given by

$$\frac{g(s)}{(s-a)^b} + h(s), \tag{10}$$

with g and h analytic over $\Re s \geq a$ and $g(a) \neq 0$. Then

$$\sum_{n\leq B} a_n = \frac{g(a)}{a(b-1)!} B^a (\log B)^{b-1}(1+o(1)). \tag{11}$$

A more sophisticated theorem is the following:

Theorem 15. *Let $(\lambda_n)_{n\in\mathbb{N}}$ be an increasing sequence of positive real numbers, and $(r_n)_{n\in\mathbb{N}}$ a sequence of positive real numbers. Suppose that the Dirichlet series $f(s)$ defined by*

$$f(s) = \sum_{n=0}^{\infty} \frac{r_n}{\lambda_n^s}$$

satisfies the following conditions:

- *the series f converges in some right half plance $\Re(s) > a > 0$;*
- *the series f has a meromorphic continuation to a half plane $\Re(s) > a - \delta_0 > 0$;*
- *in this region, it has a unique pole at $s = a$ with multiplicity $b \in \mathbb{N}$. Set $c = \lim_{s\to a} f(s)(s-a)^b > 0$;*
- *furthermore, there is a $d > 0$ such that for $\Re(s) > a - \delta_0$ we have the estimate*

$$\left| f(s)\frac{(s-a)^b}{s^b} \right| = O(|1 + \Im(s)|^d).$$

Then there is a monic polynomial P of degree $b-1$ such that for all $\delta < \delta_0$ we have

$$N(B) := \sum_{\lambda_n \le B} r_n = \frac{c}{a(b-1)!} B^a P(\log B) + O(B^{a-\delta})$$

as $B \to \infty$.

For a proof see Appendix A of [1].

We will apply Theorem 15 in the following form:

Theorem 16. *Let*

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be a Dirichlet series with an Euler product

$$F(s) = \prod_p F_p(s).$$

Suppose each Euler factor is of the form

$$F_p(s) = 1 + \frac{k}{p^s} + \sum_{l\ge 2} \frac{a_l(p)}{p^{ls}}$$

where $k \ge 1$ is an integer independent of p, and $a_l(p)$ are non-negative real numbers. Suppose there is a $\frac{1}{2} \le \delta_0 < 1$ such that for $\sigma > \delta_0$ we have

$$\sum_p \sum_{l\ge 2} \frac{a_l(p)}{p^\sigma} < +\infty.$$

Then there is a polynomial P of degree $k-1$ such that for all $\epsilon > 0$

$$\sum_{n\le B} a_n = BP(\log B) + O_\epsilon(B^{\delta_0+\epsilon})$$

as $B \to \infty$.

References

[1] Antoine Chambert-Loir and Yuri Tschinkel, Fonctions zêta des hauteurs des espaces fibrés, Rational points on algebraic varieties, Progr. Math., vol. 199, Birkhäuser, Basel, 2001, pp. 71 115.

[2] B. Datsovsky and D. J. Wright. The adelic zeta function associated with the space of binary cubic forms. II: Local theory. J. Reine Angew. Math., 367:2775, 1986.

[3] J. Denef, The rationality of the Poincaré series associated to the p-adic points on a variety. Invent. Math. 77 (1984), 1-23.

[4] M. du Sautoy, G. Taylor, The zeta function of $\mathfrak{sl}_2$ and resolution of singularities. Math. Proc. Camb. Phil. Soc. 132 (2002), no. 1, 57-73.

[5] M. du Sautoy, F. Grunewald, Analytic properties of zeta functions and subgroup growth. Ann. of Math. (2) 152 (2000), no. 3, 793-833.

[6] F.J. Grunewald, D. Segal, and G.C. Smith, Subgroups of finite index in nilpotent groups. Invernt. math. 93 (1988), 185-223.

[7] J.-I. Igusa, Some observations on higher degree characters. Amer. J. Math. 99 (1977), no. 2, 393-417.

[8] N. Kaplan, p-adic integration and subrings of $\mathbb{Z}^n$, Princeton Senior Thesis, 2007.

[9] R.I. Liu, Counting subrings of $\mathbb{Z}^n$ of index k. J. Combin. Theory Ser. A. 114 (2007), no. 2, 278-299.

[10] A. Macintyre, On definable subsets of p-adic fields. J. Symbolic Logic 41 (1976), no. 3, 605-610.

[11] J. Nakagawa, Orders of a quartic field, Mem. Amer. Math. Soc. 122 (583) (1996), viii+75.

[12] J. Shalika, R. Takloo-Bighash, and Yu. Tschinkel, Rational points on compactifications of semi-simple groups. J. Amer. Math. Soc. 20 (2007), no. 4, 1135–1186 (electronic).